Amendments to the Specification

Please replace the paragraph at page 10, lines 22-35 with the following amended paragraph:

One item of data stored in the non-volatile memory 3 of the trusted device 24 is a certificate 350. The certificate 350 contains at least a public key 351 of the trusted device 24 and an authenticated value 352 of the platform integrity metric measured by a trusted party (TP). The certificate 350 is signed by the TP using the TP's private key prior to it being stored in the trusted device 24. In later communications sessions, a user of the platform 10 can verify the integrity of the platform 10 by comparing the acquired integrity metric with the authentic integrity metric 352. If there is a match, the user can be confident that the platform 10 has not been subverted. Knowledge of the TP's generally-available public key enables simple verification of the certificate 350. The non-volatile memory 3[[5]] also contains an identity (ID) label 353. The ID label 353 is a conventional ID label, for example a serial number, that is unique within some context. The ID label 353 is generally used for indexing and labelling of data relevant to the trusted device 24, but is insufficient in itself to prove the identity of the platform 10 under trusted conditions.

Please replace the paragraph at page 12, line 27 to page 13, line 8 with the following amended paragraph:

Other integrity checks could involve establishing that various other devices, components or apparatus attached to the platform are present and in correct working order. In one example, the BIOS programs associated with a SCSI

controller could be verified to ensure communications with peripheral equipment could be trusted. In another example, the integrity of other devices, for example memory devices or co processors, on the platform could be verified by enacting fixed challenge/response interactions to ensure consistent results-this checking of the configuration of the platform is the domain of the present invention, and is discussed further below with reference to Figures 8 to 10. Where the trusted device 24 is a separable component, some such form of interaction is desirable to provide an appropriate logical binding between the trusted device ~~14~~ 24 and the platform. Also, although in the present embodiment the trusted device 24 ~~utilises~~ utilizes the data bus as its main means of communication with other parts of the platform, it would be feasible, although not so convenient, to provide alternative communications paths, such as hard-wired paths or optical paths. Further, although in the present embodiment the trusted device 24 instructs the main processor 21 to calculate the integrity metric in other embodiments, the trusted device itself is arranged to measure one or more integrity metrics.

Please replace the paragraph at page 20, lines 14-23 with the following amended paragraph:

Initially in step 800, the trusted device 24 retrieves a module configuration profile listing the identity information of the module, which may be a certificate of a public key corresponding with the module's private key. It is assumed that the trusted device 24 can verify the validation of the certificate of the module's public key. It then challenges the module by sending a nonce in step 805. After receiving the nonce, in step 810, the ~~MCA smart~~

~~card 19~~ module 15 generates and returns a response comprising the concatenation of: the plain text of the nonce, the ID 353 of the trusted device 24 and some redundancy; the signature of the plain text, generated by signing the plain text with the private key of the ~~MCA smart card 19~~ module 15; and a certificate containing the ID and the public key of the ~~MCA smart card 19~~ module 15.

Please replace the paragraph at page 20, lines 24-28 with the following amended paragraph:

The trusted device 24 authenticates the response by using the public key in the certificate to verify the signature of the plain text in step 815. If the response is not authentic, the process ends in step 820. If the response is authentic, in step 830, the authentication process executes some secure processes between the trusted device 24 and the ~~MCA smart card 19~~ module 15.

Please replace the paragraph at page 21, lines 14-28 with the following amended paragraph:

Initially, the trusted device 24 retrieves a module configuration profile listing the identity information of the module in step 1000. When the trusted device 24 meets a module 15 without a distinguishable identity, the trusted device 24 will ask for presentation of the MCA smart card 19 to confirm a valid ~~authorisation~~ authorization of the module. To do so, the trusted device first displays a message to request an MCA smart card 19 in step 1025, and second locks the user interface in step 1030. The user inserts the MCA smart card 19 in step 1033. Authentication between the trusted device 24 and the MCA smart card 19 can choose either unilateral authentication or mutual

authentication as shown above. In ~~Figure 8~~ Figure 10, we use a unilateral authentication with 2-pass, as described in ISO/IEC 9798-3. The trusted device 24 challenges the MCA smart card 19 in step 1040, and the MCA smart card 19 responds in step ~~845~~1045. The trusted device 24 authenticates the response in step 1050. If the response is not authentic, the process aborts in step 1055. If the response is authentic, the trusted device accepts the corresponding module, and the following secure process will carry on in step 1060.